C. Olivier-Anclin & Y. Zhao

TD 3 – Réseaux et sécurité des communications

Exercise 1 (Attaques sur WEP)
L'algorithme WEP (*Wired Equivalent Privacy*) était utilisé dans les premières versions de la norme IEEE 802.11 afin d'assurer la confidentialité des communications sans fil. WEP repose sur une clé secrète partagée k entre deux entités communicantes. Pour transmettre un message d, les opérations suivantes sont réalisées :

(a) génération d'un vecteur d'initialisation aléatoire iv de 24 bits ;
(b) calcul d'une somme de contrôle $c(d)$ (indépendante de la clé k) ;
(c) construction du message $P = d \,\|\, c(d)$, où $\|$ désigne la concaténation ;
(d) calcul du chiffré $C = P \oplus \mathsf{RC4}(iv, k)$, où $\oplus$ désigne le OU exclusif (XOR) ;
(e) transmission de $iv \,\|\, C$.

1. Expliquer comment un message chiffré est déchiffré puis vérifié par le destinataire.
2. Le standard WEP recommande de changer le vecteur d'initialisation à chaque message. En supposant qu'un point d'accès transmet des paquets de 1000 octets à un débit de 5 Mbit/s, calculer au bout de combien de temps un même vecteur d'initialisation sera nécessairement réutilisé. Commenter.
3. Soient P_1 et P_2 deux messages en clair (incluant leur somme de contrôle), et C_1 et C_2 les chiffrés correspondants, produits avec le même vecteur d'initialisation. Montrer que $C_2 = C_1 \oplus P_1 \oplus P_2$.
4. On suppose qu'un attaquant connaît un message en clair P_1 ainsi que le message chiffré correspondant $iv_1 \,\|\, C_1$. Montrer qu'il est alors capable de construire un chiffré valide correspondant à un message de données d_2 de son choix.
5. On suppose désormais qu'aucun message en clair n'est connu. Expliquer pourquoi l'attaque de la question précédente se généralise en une attaque par rejeu, et proposer une modification du protocole permettant d'empêcher ces attaques.

Exercise 2 (Le réseau TOR)
TOR (*The Onion Router*) est un réseau permettant d'anonymiser les communications sur Internet en rendant difficile la surveillance du trafic.

1. Sur Internet, quels sont les acteurs qui peuvent techniquement surveiller le trafic d'un utilisateur ?
2. TOR est un réseau de superposition (*overlay network*) : pour établir une route entre une source s et une destination d, la source construit un chemin aléatoire de routeurs TOR

$$(r_1, r_2, \ldots, r_n = d).$$

   Le message est chiffré de manière que chaque routeur intermédiaire r_i ne connaisse que son prédécesseur r_{i-1} et son successeur r_{i+1}, mais ni la source s (sauf pour r_1) ni la destination d (sauf pour r_{n-1}). Décrire la procédure de chiffrement appliquée par la source s pour obtenir cette propriété, et préciser le type de clés utilisées (symétriques ou asymétriques).
3. La spécification de TOR impose qu'au plus un routeur d'un même sous-réseau `/16` et au plus un routeur d'une même *famille* (routeurs administrés par la même personne, se déclarant mutuellement dans leur champ `family`) soient sélectionnés dans un circuit. Pourquoi ces contraintes sont-elles nécessaires ?
4. Lors de la construction d'un circuit, le premier routeur r_1 doit être un *nœud gardien* (*guard node*) fixe pendant plusieurs mois. Expliquer la dénomination "nœud gardien" et justifier l'intérêt cette contrainte.
5. Un attaquant contrôle un client TOR ainsi qu'un routeur TOR. Son objectif est que son routeur soit choisi comme premier nœud du circuit reliant un serveur caché au point de rendez-vous, afin de corréler le trafic de son client avec celui observé sur son routeur. Pourquoi cette position est-elle la plus intéressante pour lui ? Expliquer comment les mesures de délai sont exploitées.

Exercise 3 (Certificats Web et modèle de confiance (TLS/X.509))
Un certificat Web utilisé dans HTTPS (TLS) contient une clé publique associée à une identité (par exemple un nom de domaine), ainsi que des informations sur l'autorité qui a émis le certificat, sa période de validité et les usages autorisés.

1. Dans HTTPS moderne (TLS 1.3), la clé publique du certificat du serveur est-elle utilisée pour le chiffrement des données ou pour la signature ? Expliquer le rôle des clés éphémères.
2. Quel modèle de confiance les navigateurs utilisent-ils pour valider les certificats ? En quoi diffère-t-il du *web of trust* de PGP ?
3. Comment faut-il considérer la durée de vie d'un certificat Web et celle de la clé privée associée ?
4. Que faire si la clé privée d'un certificat serveur est compromise ? Quels mécanismes permettent aux clients d'apprendre la révocation, et quelles sont leurs limites ?
5. Expliquer le mécanisme de *certificate transparency* et en quoi il complète le modèle PKI classique.

Exercise 4 (Arithmétique modulaire appliquée aux réseaux)
On considère un serveur qui authentifie ses clients par un *token* à durée limitée : le token de la période t est

$$\tau_t = H(k\|t) \bmod 2^{32},$$

où k est une clé secrète partagée et H une fonction de hachage cryptographique (par exemple HMAC-SHA-256).

1. Un attaquant observe τ_t pour de nombreuses périodes. Expliquer pourquoi la connaissance de valeurs passées ne lui permet pas de prédire $\tau_{t'}$ pour $t' > t$.
2. Le serveur accepte le token courant τ_t mais aussi le token précédent τ_{t-1} (tolérance au décalage d'horloge). L'horloge du serveur est réinitialisée (redémarrage), de sorte que la période courante redémarre à une valeur t_0 déjà utilisée. Quel est le risque ? Proposer une contre-mesure.
3. Pour équilibrer la charge, le token est calculé sur une période de 30 secondes au lieu de 60. Sachant que la fenêtre d'usage d'un token volé est d'une période, quel est l'impact sur la sécurité et sur l'expérience utilisateur ? Discuter le compromis.
4. Un client et un serveur doivent dériver une clé de session d'un secret partagé g^{ab} (résultat d'un échange Diffie–Hellman de 2^{256} valeurs possibles) et de deux nonces de 128 bits. Expliquer pourquoi une dérivation naïve du type $\mathsf{key} = H(g^{ab})$ avec le même secret dans toutes les sessions est insuffisante, et ce que doit inclure la dérivation (KDF).